IN THE CLAIMS:

Claims 1, 6, and 11 - 26 have been cancelled. Claims 27 - 30 have been added. Claims 2 - 5 and 7 - 10 have been amended.

Claim 1 (cancelled).

2. (currently amended) The method of claim [[1]] 27, wherein addresses are TCP/IP addresses, sending an encrypted ~~or otherwise obfuscated~~ key ~~comprises~~ includes sending a packet with the encrypted ~~or otherwise obfuscated~~ key, and establishing a connection ~~comprises~~ includes establishing a connection upon receiving an acknowledgement from the ~~one or more~~ responsive nodes of the plurality of member peer nodes that successfully decrypt ~~or de-obfuscate~~ the encrypted ~~or otherwise encrypted~~ key.

3. (currently amended) The method of claim 2, wherein the connection list further includes TCP port identifiers associated with the TCP/IP addresses, to designate the port on which a member peer node corresponding to a TCP/IP address handles semi-private network traffic, and sending a packet ~~comprises~~ includes sending a packet to ~~the one or more~~ a plurality of TCP ports associated with the ~~one or more~~ plurality of member peer nodes.

4. (currently amended) The method of claim [[1]] 27, wherein the connection list further includes one or more encrypted or otherwise obfuscated keys associated with the one or more addresses on the connection list.

5. (currently amended) The method of claim [[1]] 27, wherein ~~establishing a connection comprises limiting establishing a connection to the one or more~~ the connecting member peer node cannot be connected to a same set of member peer

nodes ~~that are not connected to a same set of member peer nodes~~ as an already connected member peer node of the plurality of member peer nodes.

Claim 6 (cancelled).

7. (currently amended) The computer program product of claim [[6]] 29, wherein addresses are TCP/IP addresses, sending an encrypted ~~or otherwise obfuscated~~ key ~~comprises~~ includes sending a packet with the encrypted ~~or otherwise obfuscated~~ key, and establishing a connection ~~comprises~~ includes establishing a connection upon receiving an acknowledgement from the ~~one or more~~ responsive nodes of the plurality of member peer nodes that successfully decrypt ~~or de-obfuscate~~ the encrypted ~~or otherwise encrypted~~ key.

8. (currently amended) The computer program product of claim 7, wherein the connection list further includes TCP port identifiers associated with the TCP/IP addresses, to designate the port on which a member peer node corresponding to a TCP/IP address handles semi-private network traffic and sending a packet comprises sending a packet to ~~the one or more~~ a plurality of TCP ports associated with the ~~one or more~~ plurality of member peer nodes.

9. (currently amended) The computer program product of claim [[6]] 29, wherein the connection list further includes one or more encrypted or otherwise obfuscated keys associated with the one or more addresses on the connection list.

10. (currently amended) The computer program product of claim [[6]] 29, wherein ~~establishing a connection comprises limiting establishing a connection to the one or more~~ the connecting member peer node cannot be connected to a same set member peer nodes ~~that are not connected to a same set of member peer nodes~~ as an

already connected member peer node of the plurality of member peer nodes.

Claims 11 - 26 (cancelled).

27. (new) A method for creating a semi-private peer network, comprising:

sending an encrypted key from a connecting member peer node to a plurality of member peer nodes to connect to the plurality of peer nodes, the plurality of peer nodes corresponding to a plurality of addresses, respectively, of a connection list of addresses;

establishing a connection between the connecting member peer node and responsive nodes of the plurality of member peer nodes that successfully decrypt the encrypted key because the responsive nodes had been previously supplied with the encrypted key; and

updating an active connection list in the connecting member peer node listing the responsive nodes that successfully decrypt the encrypted key.

28. (new) The method of claim 27, wherein the connecting member peer node has a predetermined limit of responsive nodes of the plurality of member peer nodes that the connecting member peer node is connected to and does not exceed that limit.

29. (new) A computer program product including computer program code, which when executed, causes a microprocessor to perform a method for creating a semi-private peer network, the method comprising:

sending an encrypted key from a connecting member peer node to a plurality of member peer nodes to connect to the plurality of peer nodes, the plurality of peer nodes corresponding to a plurality of addresses, respectively, of a connection list of addresses;

establishing a connection between the connecting member peer node and responsive nodes of the plurality of member peer nodes that successfully decrypt the encrypted key because the responsive nodes had been previously supplied with the encrypted key; and

updating an active connection list in the connecting member peer node listing the responsive nodes that successfully decrypt the encrypted key.

30. (new) The computer program product of claim 29, wherein the connecting member peer node has a predetermined limit of responsive nodes of the plurality of member peer nodes that the connecting member peer node is connected to and does not exceed that limit.